REMARKS

In response to the Official Action dated 10/1/2007, the above-identified application has been amended to place the claims in better condition for allowance. Review and reconsideration are requested in view of the above amendments and following remarks.

The drawings were objected to as not showing all claimed features. A replacement drawing is submitted herewith. Withdrawal of the objection is kindly requested.

STATUS OF CLAIMS

Claims 1-19 stand rejected.

Claims 1-19 are appealed and claims 2-9 stand or fall with claim 1 and claims 12-19 stand or fall with claim 11.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention is summarized by referring to the specific parts of the specification and drawings. A system (FIG. 2A, page 6 lines 1-22, page 7, lines 1-22 and page 8, line 1) for increasing data access in a secure socket layer network environment includes a web server computer (102) having SSL protocol server software operably associated therewith for enabling a SSL connection, wherein SSL protocol server software includes a CA certificate and private key (page 6 lines 3-7), SSL acceleration server software operably associated with the web server computer which includes a pseudo CA certificate and access to the private key and a public key (page 6 lines 14-18). A client computer 104

(FIG. 2A,) communicatively is linked to the web server computer (102) having web browser software having SSL protocol client software operably associated therewith for enabling a first SSL connection between the client and the web server (page 6 lines 8-11), SSL acceleration client software operably associated with the client computer (104) which communicates with the SSL acceleration server software to receive a copy of the pseudo CA certificate and the public key and present the pseudo CA certificate to the web browser software for validation thereof for enabling a second SSL connection between the client computer and the web server computer in a manner which permits optimization techniques to be applied on data transmitted through the second SSL connection (page 6 lines 19-22, page 7, lines 1-22 and page 8, line 1).

A method for increasing data access in a secure socket layer network environment (FIG. 2A, FIG. 2B) includes the steps of employing a web server computer (102) having SSL protocol server software operably associated therewith for enabling a SSL connection (page 6 lines 3-7), wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with the web server computer which includes a pseudo CA certificate and access to the private key and a public key(page 6 lines 14-18); and

employing a client computer (104) communicatively linked to the web server computer (102) having web browser software having SSL protocol client software operably associated therewith for enabling a first SSL connection between the client (104) and the web server (104), SSL acceleration client software operably associated with the client computer which communicates with the SSL acceleration server software to

receive a copy of the pseudo CA certificate and the public key and present the pseudo CA certificate to the web browser software for validation thereof for enabling a second SSL connection between the client computer and the web server computer in a manner which permits optimization techniques to be applied on data transmitted through the second SSL connection (page 6 lines 19-22, page 7, lines 1-22 and page 8, line 1).

GROUND OF REJECTION TO BE REVIEWED OR APPEALED

1. Whether the specification and claims 1-19 fail to comply with the written description requirement under 35 U.S.C. § 112, first paragraph.

1. Whether claims 1-19 are unpatentable under 35 U.S.C. §103(a) as obvious over United States Patent No 6643701 to Aziz et al. in view of United States Publication 2003/0046532 to Gast and/or in view of Freed et al. United States Publication 2003/0014628.

ARGUMENT

An issue is whether the specification and claims 1-19 fail to comply with the written description requirement under 35 U.S.C. § 112, first paragraph.

Another issue is whether claims 1-19 are unpatentable under 35 U.S.C. §103(a) as obvious over United States Patent No 6643701 to Aziz et al. in view of United States Publication 2003/0046532 to Gast and/or in view of Freed et al. United States Publication 2003/0014628.

Stampede Technologies, Inc. is a leader in software development in the area of accelerating data over various networks. Numerous independent articles recognize Stampede Technologies, Inc. as a leader in the field of enhancing communication over networks, such as the Internet, see for example, http://www.javascriptsearch.com/news/news/070214StampedeApplicationAcceleration.html , http://www.econtentmag.com/Articles/ArticleReader.aspx?ArticleID=7246 , http://ajax.sys-con.com/read/324139.htm , http://cincinnati.dbusinessnews.com/shownews.php?newsid=107850&type_news=past.

The Examiner's Rejections under 35 U.S.C §112

In response to a non-final Office Action dated 3/13/2007, applicant amended the claims which the Examiner indicated triggered a rejection under 35 U.S.C. § 112 that the claims and specification did not provide support for the claimed language as previously submitted.

Specifically, the examiner stated:

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The specification fails to provide proper antecedent basis for the recitations of *"a first SSL connection between said client and said web server"*, *"a second SSL connection between said client and said server in a manner which permits optimization techniques to be performed on data transmitted through said second SSL connection"*, *"means for permitting establishing a first SSL connection...and permitting a second SSL connection"*, and *"means for establishing said first SSL connection and... for enabling said second SSL connection between said client and said server in a manner which permits optimization techniques to be performed on data transmitted through said second SSL connection"*.

Claims 1 - 19 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Applicant has not pointed out where the new (or amended) claim is supported, nor does there appear to be a written description of the claim limitations in the application as filed (see above objection to the specification).

Applicants noted that the phrase "performed on data" appeared to be the language objectionable in the claims and moved to amend the claims by replacing this language with "applied on data". Further, Applicants moved to amend the phrase "means for

permitting establishing" to "means for enabling". These amendments were submitted to be a change in similar words, and to accommodate the examiner's position Applicants provided the identical terms used in the specification as opposed to similar words conveying similar meaning and were not of a type of change which would trigger a change in scope of claim interpretation.

Applicants set forth the pertinent parts of the originally filed specification which were italicized in part to demonstrate the claimed language is clearly supported as well as the amended language to the specification submitted herewith. Comments are in bold and bracketed.

At page 6, lines 1-22, page 7, lines 1-22 and page 8, lines 1-2 of the filed Specification, the following is stated:

> The present invention is generally depicted in FIGS. 2A and 2B and is directed to a system and method for increasing data access in a secure socket layer network environment and is generally designated by the number 100. The system 100 includes a *web server computer 102* which has an operating system/software, server software, memory and linking devices as is known in the art. Further, the *computer 102 has SSL protocol server software operably disposed thereon for enabling a SSL connection, wherein SSL protocol server software includes a CA certificate and private key.*
>
> A *client computer 104* includes an operating system/software, web browser software having SSL protocol client software operably disposed *thereon for enabling a SSL connection*, memory and linking devices as is known in the art and is communicatively linked to the web server computer 102. SSL acceleration client (SSLAC) software is operably disposed on the client computer 104 for monitoring when the web browser requests a SSL connection with the web server 102.
>
> *SSL acceleration server (SSLAS) software is operably disposed on the web server computer 104 for receiving a request for a SSL connection through SSL acceleration client software.* The SSL acceleration server software is operably associated with the SSL protocol server software to obtain one either a copy or an equal credential of the CA certificate (i.e., a pseudo CA certificate) and private key.
>
> The operation of the invention can be understood from steps shown in

FIGS. 2A and 2B. *SSL acceleration client software intercepts 200 new SSL request for a SSL secure connection from the web browser to a target web server. The SSL acceleration client software then initiates 202 a SSL handshake with the SSLAS operably associated with the target web server computer and to start SSL connection.* The SSLAS then determines 204 which CA certificate is operably associated with the target web server. As part of the SSL handshake between SSLAC and SSLAS, the SSLAS sends 206 this CA certificate to SSLAC along with a public key. *At this point a secure SSL session is established between SSLAC and SSLAS and all subsequent data traffic between SSLAC and SSLAS flows over this secure connection.* **[i.e., a first SSL connection]** *The SSLAC software sends 208 the copy of the CA certificate to the web browser for validation 210. Web browser software sends 212 a list of available encryption algorithms (ciphers) back to target web server (i.e., server computer 102). SSLAC software intercepts this from the browser and sends 214 a chosen cipher to the browser software. The web browser software creates 216 a secret key, encrypts using chosen cipher and using the previously received public key and sends 218 the encrypted secret key to the target server, which is intercepted and sent 219 through the SSL acceleration client software to the SSLAS software. SSLAS software de-encrypts 220 the secret key using the private key operably associated with the target server. SSLAS software sends 222 decrypted secret key back to SSLAS software via the secure SSL connection, wherein a "handshake" is completed and secure communications between the client computer's web browser and SSLAS software* **[i.e., a second SSL connection]** *and by using the secret key, data can be accelerated between the client computer 104 and the web server computer 102 employing acceleration software, such as compression software of the SSL acceleration client/server software.*

Because the SSL connection is terminated by SSLAC, *SSLAC can process the data in unencrypted form allowing it to apply data compression and other optimization techniques to the data stream.* This is done in such a way that the credentials of the SSLAS are presented to the web browser without having violated the SSL paradigm because the private key of the SSLAS was never transmitted to SSLAC.

It has been submitted that the originally filed specification clearly discloses a client computer, web server, first and second SSL connections wherein the second permits optimization techniques to be applied on the data transmitted through the second SSL connection. There is also clearly disclosed means for enabling each connection.

The Examiner did not enter the amendment because there was a typographical in the Remarks section of Applicant's remarks which inadvertently referred to the "second SSL connection" as a "first SSL connection". This was the only apparent reason posed for non-entry of the amendment. Accordingly, entry of the amendment and the rejection to the specification and claims is requested to be reversed and withdrawn.

Stated Grounds of Rejection by Examiner under 35 U.S.C § 103

In the Final Office Action dated 10/1/2007, the Examiner rejected to Claims 1-19. The Examiner stated:

> **Claims 1 – 8 and 10 – 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz et al. (Aziz), "Method and Apparatus for Providing Secure Communication with a Relay in a Network", U.S. Patent 6,643,701 in view of Gast, "System and Method for Accelerating Cryptographically Secured Transactions", U.S. Patent Publication 2003/0046532.**

As to Claim 1, the Examiner asserts Aziz discloses first and second SSL connections between a client and server and a web server computer having SSL protocol server software as claimed and a client computer having web browser software having SSL protocol software as claimed, but does not include SSL acceleration software and cites Gast in this regard. It is asserted that it would have been obvious to one skilled in the art to recognize the benefits of acceleration of Gast within the system of Aziz.

Reasons Why Examiner's Assertion is Incorrect

The Nonobviousness Requirement - 35 U.S.C. §103

35 U.S.C. § 103 states a patent may not be obtained though the invention is not identically disclosed or described as set forth title 35 USC § 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The Supreme Court recently addressed the issue of obviousness in KSR International Co. v. Teleflex Inc., 127 S. Ct. 1727 (2007). The Court stated that the Graham v. John Deere Co. of Kansas City, 383 U.S. 1 (1966), factors still control an obviousness inquiry. Those factors are: 1) "the scope and content of the prior art"; 2) the "differences between the prior art and the claims"; 3) "the level of ordinary skill in the pertinent art"; and 4) objective evidence of nonobviousness. KSR, 127 S. Ct. at 1734 (quoting Graham, 383 U.S. at 17-18). Moreover, the Court indicated that there is "no necessary inconsistency between the idea underlying the TSM test and the Graham analysis." Id. As long as the test is not applied as a "rigid and mandatory" formula, that test can provide "helpful insight" to an obviousness inquiry. KSR, 127 S. Ct. at 1731; Takeda Chemical Industries, Ltd. v. Alphapharm Pty., Ltd., No. 06-1329 (Fed. Cir. June 28, 2007). It is also stated that "where an application claims a structure already known in the prior art that is altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result". KSR, at 1739. In other words, if a person of ordinary skill can

implement a predictable variation of known components, § 103 likely bars its patentability. KSR was concerned with substitution of a known component having a known function and substituting it into another invention for performing the same function.

At the outset, it is important to note how this case is not the same as the much publicized KSR case. KSR, 127 S.Ct. at 1740. Here, the applicant points out quite clearly that the art cited is deficient in lacking the claimed structure. There are indeed claimed differences between the prior art and the claims. At the time of the invention, the level of skill in the art has not been shown to have developed as to the art nor as to any like claimed structure or disclosure in the cited art. The only evidence of record which has been offered at this time tilts toward patentability. The Court held in Graham v. John Deere Co., 383 U.S. 1 (1966):

> While the ultimate question of patent validity is one of law, ... the § 103 condition, which is but one of three conditions, each of which must be satisfied, lends itself to several basic factual inquiries. Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented. As indicia of obviousness or nonobviousness, these inquiries may have relevancy.
>
> This is not to say, however, that there will not be difficulties in applying the nonobviousness test. What is obvious is not a question upon which there is likely to be uniformity of thought in every given factual context.

383 U.S. at 17-18 (citations omitted).

The Court also instructed that the standard set forth in Graham would go beyond an inquiry of purely technical issues:

> These legal inferences or subtests do focus attention on economic and motivational rather than technical issues and are, therefore, more susceptible of judicial treatment than are the highly technical facts often present in patent litigation.... Such inquiries may lend a helping hand to the judiciary which, as Mr. Justice Frankfurter observed, is most ill-fitted to discharge the technological duties cast upon it by patent legislation. ...They may also serve to "guard against slipping into use of hindsight," ... and to resist the temptation to read into the prior art the teachings of the invention in issue. 383 U.S. at 35-36 (citations omitted).

Thus, under Graham, the obviousness inquiry is highly fact specific, and requires an examination of the above stated factors.

Stampede Technologies, Inc. set out to reduce traffic over the network and increase the speed in which data is transmitted over the network when faced with an environment using single SSL connections between the same client server pairing.

Prior Art at time of the Invention

The cited art references in this case are United States Patent No. 6643701 to Aziz et al. in view of United States Publication 2003/0046532 to Gast and in view of Freed et al. United States Publication 2003/0014628. No other reference is cited in combination therewith to render obvious claims 1, 10 and 11 and the claims which depend therefrom.

Prior to the claimed invention, the prior art provided for establishing a single SSL connection between a same client and server pair through which an established communication transmitted data over such connection using an established certificate. Each prior art paradigm fails to show multiple SSL connections established between the same client and server wherein a given certificate and a copy of the certificate are employed.

Aziz only discloses making a single connection between each client and a relay and a relay and a server. Aziz states that the connection can be a cleartext HTTP connection (non-secure).

Gast is directed to a system and method for accelerating cryptographically secured transactions. Gast is concerned with offloading encryption processing to central encryption servers equipped with hardware built to accelerate encryption speed and reduce encryption latency.

Freed et al. discloses a secure sockets layer architecture which employs an intermediate device between the client computer and the server computer which intercepts SSL/TCP data and then performs one or more transactions to aid in acceleration.

Differences between the Claimed Invention and Art

Neither Aziz, Gast or Freed et al. alone or together disclose, suggest or teach the invention nor do any provide a teaching, suggestion or motivation to perform the method of instant claimed invention. It is only the Examiner's opinion as to what the cited references teach, suggest or disclose and this has been refuted by Applicants specifically pointing out the scope of the art, differences between the references and the instant invention and the level of skill in the art at that time.

Aside Aziz, Gast or Freed et al. which Applicants assert do not teach, disclose or suggest the invention, no other evidence has been put forth which teaches, suggests or discloses the invention. Applicants provided adequate evidence to rebut the examiner's

contention via arguments and the Declaration of record.

In addressing the first factor cited above, it is respectfully submitted that the cited art, namely, Aziz, Gast or Freed et al., do not render obvious the instant invention, to produce the claimed present invention. A person of ordinary skill in the field for making a system or method of using a system for increasing data access in a secure socket layer network environment as with the instant invention at the time of the invention would not have reasonably looked at Aziz, Gast nor Freed et al. and been able to derive the claimed invention.

Combining Aziz, Gast or Freed et al. teachings at best provide for a system for offloading encryption latency issues using single SSL connections between a server, relay and client computer. As can be seen from their combined specification and claims, this does no more than teach of single conventional SSL connection techniques between the same client and server pairing using a given certificate.

The Examiner failed to correctly appreciate and consider all of the limitations in the claimed invention as properly interpreted in light of the applicants' specification.

Claim 1 calls for a system for increasing data access in a secure socket layer network environment, which includes:

a web server computer having SSL protocol server software operably associated therewith for enabling a SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with the web server computer which includes a pseudo CA certificate and access to the private key and a public key; and

a client computer communicatively linked to the web server computer having web browser software having SSL protocol client software operably associated therewith for enabling a first SSL connection between the client and the web server, SSL acceleration client software operably associated with the client computer which communicates with the SSL acceleration server software to receive a copy of the pseudo CA certificate and the public key and present the pseudo CA certificate to the web browser software for validation thereof for enabling a second SSL connection between the client computer and the web server computer in a manner which permits optimization techniques to be applied on data transmitted through the second SSL connection.

Claim 10 calls for a system for increasing data access in a secure socket layer network environment, which includes:

a web server computer having a means for enabling a first SSL connection and SSL acceleration server software for transferring a copy of a pseudo CA certificate and a public key and permitting establishing a second SSL connection; and

a client computer communicatively linked to the web server computer having means for enabling the first SSL connection and having SSL acceleration client software operably associated with the client computer which communicates with the SSL acceleration server software to receive the copy of a pseudo CA certificate and the public key and present the pseudo CA certificate to web browser software on the client computer for validation thereof and for enabling the second SSL connection between the client computer and the web server computer in a manner which permits optimization techniques to be applied on data transmitted through the second SSL connection.

Claim 11 calls for a method for increasing data access in a secure socket layer network environment, which includes the steps of:

employing a web server computer having SSL protocol server software operably associated therewith for enabling a SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with the web server computer which includes a pseudo CA certificate and access to the private key and a public key; and

employing a client computer communicatively linked to the web server computer having web browser software having SSL protocol client software operably associated therewith for enabling a first SSL connection between the client and the web server, SSL acceleration client software operably associated with the client computer which communicates with the SSL acceleration server software to receive a copy of the pseudo CA certificate and the public key and present the pseudo CA certificate to the web browser software for validation thereof for enabling a second SSL connection between the client computer and the web server computer in a manner which permits optimization techniques to be applied on data transmitted through the second SSL connection.

Aziz does not teach disclose or suggest, SSL acceleration client software operably associated with the client computer which communicates with the SSL acceleration server software to receive a copy of the pseudo CA certificate and the public key and present the pseudo CA certificate to the web browser software for validation thereof for enabling a second SSL connection between the same client computer and the same web server computer in a manner which permits optimization techniques to be applied on data

transmitted through the second SSL connection.

Rather, the Examiner has composed an incomplete set of pieces of art in an effort to assemble a system to render an obviousness rejection. However, no cutting and pasting of such pieces can in any way do so.

Aziz only discloses making a single connection between each client and a relay and a relay and a server. Aziz states that the connection can be a cleartext HTTP connection. This, however, can be a problem and create a security issue because Basic credentials are Base64-encoded. If Basic credentials are sent over an HTTP connection, they may be read as clear text and decoded.

There is no disclosure, suggestion or teaching in Aziz as to the need or means for making multiple SSL connections with the same client and server. Nor is there any disclosure, teaching or suggestion of SSL acceleration server software operably associated with a web server computer which includes a pseudo CA certificate and access to a private key and a public key and a client computer communicatively linked to the web server computer having web browser software having SSL protocol client software operably associated therewith for enabling a first SSL connection between the client and the web server, SSL acceleration client software operably associated with the client computer which communicates with the SSL acceleration server software to receive a copy of the pseudo CA certificate and said public key and present the pseudo CA certificate to the web browser software for validation thereof for enabling a second SSL connection between the client computer and said web server computer in a manner which permits optimization techniques to be applied on data transmitted through said second

SSL connection. This is only taught by the present invention.

Gast is directed to a system and method for accelerating cryptographically secured transactions. Gast is concerned with offloading encryption processing to central encryption servers equipped with hardware built to accelerate encryption speed and reduce latency [see paragraph 0015 of Gast]. Gast simply moves the task of processing the security mechanism, i.e., establishing a SSL session to a central control point [0022]. The point stressed in Gast is to offload the establishment of SSL connections by the server, not to establish additional SSL connections between the same client and server pairing. In contrast, the instant invention provides a CA certificate and a pseudo CA certificate to establish concurrent SSL connections whereby data can pass in a compressed form, for example, in the second established connection.

Applicants assert Gast teaches away from the instant invention. The Examiner asserts that Gast does not a teaching away from the instant invention.

It is recognized that teaching away requires discouragement of the invention. What a reference teaches or suggests must be examined in the context of knowledge, skill and reasoning ability of a skilled artisan. Gast recognizes the problem of encryption latency, paragraph [0015] of Gast. This latency can be encountered between a client server relationship. Gast chooses to offload the cryptographic process to central cryptographic hardware component employing an intermediary device to deal with the issue as opposed to creating an additional potential encryption latency issue between a server and client.

The concept presented by the instant invention is in creating multiple SSL direct

connections between the same client and server is discouraged by the prior art with the recognition of such connections causing encryption latency issues. Further, there is no teaching of how to create such direct multiple SSL connections between the same client and server in a manner to enhance performance and deal with latency issues directly between the same client and server employing a given CA certificate and a pseudo copy thereof.

Aziz attempts teaches toward offloading the SSL connection by using a cleartext HTTP connection, i.e., Aziz states this reduces the server workload even more compared to using previously negotiated SSL sessions." Combining the references in no way would result in the present invention. In fairly interpreting the teachings of each reference and combining such teachings, a reasonable combination might result in the combination of offloading encryption processing further with the aid of relays. This does not render the instant invention.

Like Aziz, in Freed et al. there is no direct link between the client computer and the server computer. As seen in paragraphs [0007-0010] of Freed et al., there is merely a conventional SSL handshake which is employed and all secure data is sent through the one secure tunnel which is created. Freed et al. are concerned with offloading the server the task of encryption/decryption task by employing a tertiary or intermediary device to interact with the client and the server. Nevertheless, the tertiary computer employs conventional handshake technology.

This is very different from the instant invention. The instant invention provides a server with SSL protocol server software and SSL acceleration server software on both

the client and server for enabling direct and multiple SSL sessions to take place through the use of creating a pseudo CA certificate on the web server in addition to having the existing CA certificate on the web server which are presented to the client computer having SSL protocol and SSL acceleration software thereon. By so providing, multiple direct secure links are created. Freed et al., like Aziz, introduces a third element in the chain of connection and another potential break point for communication.

The instant invention enables secure data be transacted using the CA certificate from the web server over an initial SSL connection for transacting key data which must pass over such connection, such as when connecting to a secure bank site, for example. In addition, the instant invention provides the pseudo CA certificate and secondary SSL connection through which data may pass in a secure connection which enables functional operations (optimization techniques) to be performed thereon, such as compression of data. This is not taught, disclosed or suggested in Freed et al. (or Aziz) and this can't be accomplished in the teachings of Freed et al or Aziz. Freed et al. only acts as an intermediary intercepting all communication over the existing SSL connection and passes the data accordingly, paragraph [0039]. Paragraphs [0052] - [0053] and the claims in Freed et al. further illustrate Freed et al. are only concerned with providing a classic SSL connection between the client and server through an intermediary device.

Applicants 132 Declarations filed on 4/12/2007 and 2/1/2008 further illustrate the novelty and nonobviousness of the instant invention. There is no reasonable basis in which the references can be construed to teach, suggest or disclose the instant invention.

The issue is here is whether Aziz, Gast nor Freed et al. and some other knowledge

(presumably the Examiner's) brought here together renders obvious claimed invention. The Federal Circuit has followed the Court's holding in Adams. See, e.g., Kahn v. General Motors Corp., 135 F.3d 1472, 1479-80 (Fed. Cir. 1998), cert. denied, 525 U.S. 875 (1998) ("In determining obviousness, the invention must be considered as a whole.").

The differences between the prior art and claimed invention are very apparent, i.e., enabling secure data be transacted using the CA certificate from the web server over an initial SSL connection for transacting key data which must pass over such connection, and providing the pseudo CA certificate and secondary SSL connection through which data may pass in a secure connection which enables functional operations (optimization techniques) to be performed thereon. The level of ordinary skill in the art in the field of field has not been established or demonstrated by the examiner and cannot be asserted without some reasonable basis for doing so. Finally, while secondary considerations were not vigorously stressed in the prosecution of the application, it is noted that the applicant's invention has enjoyed much commercial success and is of wide spread need in the industry.

The instant invention is respectfully submitted to be patentably distinct over the art of record. Withdrawal of the rejection of the rejection of claims under 35 U.S.C. 103 over Aziz in view of Gast and/or Freed et al. and allowance of claims 1-19 are respectfully respectfully requested.

Respectfully submitted,

/R. William Graham/

R. William Graham

Reg. No. 33,891

Certificate of transmission

I hereby certify that this correspondence is being electronically filed with the Commissioner of Patent and Trademarks, Washington, D.C. 20231on the date shown below.

Date. April 1, 2008

R. William Graham